APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,411	02/12/2002	Roger Eastvold	390P010777-US (PAR)	7013

7590 06/12/2006	EXAMINER
Geza C. Ziegler, Jr. PERMAN & GREEN, LLP 425 Post Road Fairfield, CT 06430	PATEL, ASHOKKUMAR B

ART UNIT	PAPER NUMBER
2154	

DATE MAILED: 06/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
	10/074,411	EASTVOLD, ROGER
Office Action Summary	Examiner	Art Unit
	Ashok B. Patel	2154

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>31 March 2006</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-23</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-23</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-23 are subject to examination.

Continued Examination Under 37 CFR 1.114

2.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

03/31/2006 has been entered.

Response to Arguments

3.   Applicant's arguments with respect to claims 1-23 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5.   Claims 1, 6, and 11 are rejected under 35 U.S.C. 112, first paragraph, as failing

to comply with the written description requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to reasonably convey to

one skilled in the relevant art that the inventor(s), at the time the application was filed,

had possession of the claimed invention. These claims contains the phrase " send a

different data" to the local network, is not described in the specification. How the data is

different? How is it related to other claim limitations?

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 102

6.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless-

> (e) the invention was described in (1) an application for patent, published under section 122(b), by
> another filed in the United States before the invention by the applicant for patent or (2) a patent
> granted on an application for patent by another filed in the United States before the invention by the
> applicant for patent, except that an international application filed under the treaty defined in section
> 351(a) shall have the effects for purposes of this subsection of an application filed in the United States
> only if the international application designated the United States and was published under Article 21(2)
> of such treaty in the English language.

7.   Claims 1, 2, 4-7, 9-13, 15-23 are rejected under 35 U.S.C. 102(e) as being

anticipated by Crist et al. (hereinafter Crist) (US 6, 879, 940 B1)

Referring to claim 1,

Crist teaches a system for accessing data remotely from a network, comprising:

a local network interface permitting data transfer (Fig. 3, element 36, "Host

Network", col. 7, line 8-10, "Additionally, the particular client may only connect to their

local workstation 32 after being screened by the host's security system.") between a

local network (Fig. 3, elements 34, 11) and an intermediate network (Fig. 3, elements

32, col. 7, line 12-17, "The host schedules particular times on the test system 34 for

particular single clients, who may then operate the test system 34 as described in the

first embodiment. A switch matrix 33, is provided so that a host network 36 may

connect or disconnect from the test system 34 as described in the previous embodiment.");

a remote network interface device (Fig. 3, element 30, "Remote Workstation", col. 5, line 7-33) permitting data transfer between the intermediate network (Fig. 3, elements 32, col. 7, line 12-17), and a remote network (col. 5, line 7-33); and

a module located within the intermediate network through which all data transferring between the local network and the remote network must pass, the module being configured to receive and process data from the remote network and send a different data to the local network based on the data received from the remote network. (col. 6, line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is desirable because of the large quantity of data that must be transferred to and from the test system 8.")

Referring to claim 2,

Crist teaches the system of claim 1, wherein the data transfer between each of the networks occurs via the Internet Protocol (IP), and wherein each network has its own unique IP address. (col. 5, line 7-33)

Referring to claim 4,

Crist teaches the system of claim 1, wherein the module exchanges data with an equipment diagnostic monitor system located within the intermediate network, and wherein the equipment diagnostic monitor system has the function of monitoring tests

performed on at least one tool residing within the local network (col. 6, line 1-3, "The

test program must at some point in time be transferred to the local workstation 7 in

order to run the test system 8 from the local workstation 7. In this embodiment, the test

system 8 is connected to the host's network 10 (LAN). The local workstation 7 is

desirable because of the large quantity of data that must be transferred to and from the

test system 8.").

Referring to claim 5,

Crist teaches the system of claim 4, wherein the equipment diagnostic monitor

system collects and analyzes data from tests performed on the at least tool. (col. 6, line

1-3, "The test program must at some point in time be transferred to the local workstation

7 in order to run the test system 8 from the local workstation 7. In this embodiment, the

test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is

desirable because of the large quantity of data that must be transferred to and from the

test system 8.", col. 4, line 15-21).

Referring to claim 6,

Crist teaches a system for accessing a local network from a remote network through an

intermediate network , comprising:

a local network interface permitting data transfer (Fig. 3, element 36, "Host

Network", col. 7, line 8-10, "Additionally, the particular client may only connect to their

local workstation 32 after being screened by the host's security system.") between a

local network (Fig. 3, elements 34, 11) and the intermediate network (Fig. 3, elements

32, col. 7, line 12-17, "The host schedules particular times on the test system 34 for

particular single clients, who may then operate the test system 34 as described in the first embodiment. A switch matrix 33, is provided so that a host network 36 may connect or disconnect from the test system 34 as described in the previous embodiment.");

a remote network interface device (Fig. 3, element 30, "Remote Workstation", col. 5, line 7-33) permitting data transfer between the remote network (Fig. 3, elements 32, col. 7, line 12-17), and the intermediate network (col. 5, line 7-33);

a module located within the intermediate network, the module being configured to receive and process data from the remote network and send a different data to the local network based on the data received from the remote network (col. 6, line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is desirable because of the large quantity of data that must be transferred to and from the test system 8."); and

an equipment diagnostic monitor system for monitoring the health of equipment within the local network, the equipment diagnostic monitoring system being located within the intermediate network, wherein the equipment diagnostic monitor system monitors tests performed on at least one item residing within the local network (col. 6, line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local

workstation 7 is desirable because of the large quantity of data that must be transferred

to and from the test system 8.")

Referring to claim 7,

Crist teaches the system of claim 6, wherein the data transfer between each of the

networks occurs via the Internet Protocol (IP). (col. 5, line 7-33).

Referring to claim 9,

Crist teaches the system of claim 6, wherein the equipment diagnostic monitor system

collects and analyzes data from the tests performed on the at least one item. (col. 6, line

1-3, col. 4, line 15-21)

Referring to claim 10,

Crist teaches the system of claim 6, wherein a user on the remote network may request

that tests be performed on the at least one item, and may upload data to the remote

network, from the tests performed on the at least one item. (Abstract)

Referring to claim 11,

Crist teaches a data system (Fig. 4), comprising:

a local network interface device (Fig. 3, element 36, "Host Network", col. 7, line

8-10, "Additionally, the particular client may only connect to their local workstation 32

after being screened by the host's security system.") enabling data transfer between a

local network (Fig. 3, elements 34, 11) and an intermediate network ((Fig. 3, elements

32, col. 7, line 12-17, "The host schedules particular times on the test system 34 for

particular single clients, who may then operate the test system 34 as described in the

first embodiment. A switch matrix 33, is provided so that a host network 36 may

connect or disconnect from the test system 34 as described in the previous embodiment.");

a remote network interface device (Fig. 3, element 30, col. 5, line7-33) enabling data transfer between a remote network (col. 5, line 7-33) and the intermediate network Fig. 3, element 32, col.7, line 12-17) ; and

an equipment diagnostic monitor system for monitoring the health of equipment within the local network, the equipment diagnostic monitoring system being located within the intermediate network, wherein the equipment diagnostic monitor system monitors tests performed on at least one item in the local network (col. 6, line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is desirable because of the large quantity of data that must be transferred to and from the test system 8.")

wherein the intermediate network is configured to receive and selectively process data from the remote network depending on a set of predetermined criteria applied by the intermediate network and send a different data to the local network based on the selectively processed data.(col. 6, line 57 through col. 7, line 17).

Referring to claim 12,

Crist teaches the system of claim 11, further comprising a security module located within the intermediate network, through which all data transferring between the local network and the remote network must pass. (Fig. 3, element 33).

Referring to claim 13,

Crist teaches the system of claim 12, wherein data transfer between each of the networks occurs via the Internet Protocol (IP). (col. 5, line 7-33).

Referring to claim 15,

Crist teaches the system of claim 11, wherein the equipment diagnostic monitor system collects and analyzes data from tests performed on the at least one item. (col. 6, line 1-3, col. 4, line 15-21)

Referring to claim 16,

Crist teaches the system of claim 11, wherein the equipment diagnostic monitor system is configured to execute or ignore a request by a user on the remote network based on a set of predetermined criteria, wherein the user requests that tests be performed on the at least one item, and that data from previous tests performed on the at least one item be uploaded (col.6, line 38-47, col. 6, line 57 through col. 7, line 17).

Referring to claim 17,

Crist teaches the system of claim 11, wherein a user on the remote network sends a suggestion regarding the operation of the at least one item being monitored to an entity managing the item on the local network. (col. 6, line14-38)

Referring to claim 18,

Crist teaches the system of claim 11, wherein the equipment diagnostic monitor system sends an alert to a predetermined entity when the analysis of tool data indicates that the at least one item is operating outside of a predetermined performance range. (col. 4, line 15-21)

Referring to claim 19,

Crist teaches the system of claim 1 further comprising a remote control proxy server in the intermediate network that is between the local network and the remote network that prevents direct IP routing to a device in the local network that is being accessed by the remote network.(Fig. 3, element 36)

Referring to claims 20, 21 and 22,

Crist teaches the system of claim further comprising a semiconductor tool coupled to the local network, a user being able to access the semiconductor tool via the remote network, and the system of claim 20, wherein the intermediate network further comprises an equipment diagnostic monitor system that monitors and analyzes the semiconductor tool, and the system of claim 21, wherein the equipment diagnostic monitor system controls tests performed by software within the semiconductor tool, saves data from the tests and sends out alerts to a remote user via the remote network when the semiconductor tool is operating outside a predetermined performance range. (col.4, line15-21, col. 6, line 1-3, col. 6, line 57 through col. 7, line 17)

Referring to claim 23,

Crist teaches the system of claim 21, wherein the equipment monitor system effects access to the semiconductor tool by a remote user. (col. 6, line 57 through col. 7, line 17)

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9.   Claims 3, 8 and 14 are rejected under 35 U.S.C. 103(a) as being Crist et al. (hereinafter Crist) (US 6, 879, 940 B1) in view of Reid et al. (hereinafter Reid)(US 6, 182, 226 B1)

Referring to claim 3,

Keeping in mine the teachings of Crist as stated above, Crist explicitly fails to teach the system of claim 2, wherein the module hides the IP addresses of the remote network and the local network from each other.

Reid teaches "A rewrite node is a point in an access rule where source or destination addresses are mapped to other source or destination addresses. Destination IP address rewrites allow an inbound connection through network address translation (NAT) address hiding to be remapped to a destination inside the NAT barrier. Source address rewrites can be used on outbound connections to make the source appear to be one of many external addresses. This process allows the internal hosts to be aliased to external addresses. Rewrites can be based on any connection criteria, including users.", col. 6, lines 46-56. (wherein the data transfer between each of the networks occurs via the Internet Protocol (IP), and wherein each network has its own unique IP address, and the system of claim 2, wherein the module hides the IP addresses of the remote network and the local network from each other.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to add the teachings of the Reid to the firewalls of the service facility of Crist such that address rewrites for inbound and outbound can be implemented based on any connection criteria, including users.

It would have been obvious because it provides a method for controlling interactions between networks by the use of firewalls with defined regions as taught by Reid.

Referring to claim 8,

Keeping in mine the teachings of Crist as stated above, Crist explicitly fails to teach the system of claim 7, wherein the module hides the IP addresses of the local network and the remote network from each other.

Reid teaches "A rewrite node is a point in an access rule where source or destination addresses are mapped to other source or destination addresses. Destination IP address rewrites allow an inbound connection through network address translation (NAT) address hiding to be remapped to a destination inside the NAT barrier. Source address rewrites can be used on outbound connections to make the source appear to be one of many external addresses. This process allows the internal hosts to be aliased to external addresses. Rewrites can be based on any connection criteria, including users.", col. 6, lines 46-56. (wherein the data transfer between each of the networks occurs via the Internet Protocol (IP), and wherein each network has its own unique IP address, and the system of claim 2, wherein the module hides the IP addresses of the remote network and the local network from each other.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to add the teachings of the Reid to the fire wall of the service facility of Crist such that address rewrites for inbound and outbound can be implemented based on any connection criteria, including users.

It would have been obvious because it provides a method for controlling interactions between networks by the use of firewalls with defined regions as taught by Reid.

Referring to claim 14,

Keeping in mine the teachings of Crist as stated above, Crist explicitly fails to teach the system of claim 13, wherein the module hides the IP addresses of the local network and the remote network from each other.

Reid teaches "A rewrite node is a point in an access rule where source or destination addresses are mapped to other source or destination addresses. Destination IP address rewrites allow an inbound connection through network address translation (NAT) address hiding to be remapped to a destination inside the NAT barrier. Source address rewrites can be used on outbound connections to make the source appear to be one of many external addresses. This process allows the internal hosts to be aliased to external addresses. Rewrites can be based on any connection criteria, including users.", col. 6, lines 46-56. (wherein the data transfer between each of the networks occurs via the Internet Protocol (IP), and wherein each network has its own unique IP address, and the system of claim 2, wherein the module hides the IP addresses of the remote network and the local network from each other.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to add the teachings of the Reid to the fire wall of the service facility of Crist such that address rewrites for inbound and outbound can be implemented based on any connection criteria, including users.

It would have been obvious because it provides a method for controlling interactions between networks by the use of firewalls with defined regions as taught by Reid.

Conclusion

Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (571) 272-3972. The examiner can normally be reached on 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A. Follansbee can be reached on (571) 272-3964. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abp
***

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100